

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья

УДК 347.3/7
https://doi.org/10.23947/2949-1843-2023-1-1-126-136

Кибepпреступления: понятие, классификация, международное противодействие


С. С. Витвицкая, А. А. Витвицкий, Ю. И. Исакова
Донской государственный технический университет, Российская Федерация,
г. Ростов-на-Дону, пл. Гагарина, 1
✉ omar67@yandex.ru



Аннотация

Введение. В уголовно-правовой доктрине, нормативных источниках и официальных документах, принятых на международном уровне, существуют различные подходы к определению понятий «киберпреступность» и «киберпреступления», предлагаются разные перечни и классификации этих преступных деяний. Эти разночтения отрицательно сказываются на результативности борьбы с данной разновидностью преступлений. Трансграничный характер киберпреступлений и взаимосвязанность информационно-телекоммуникационных технологий и информационных инфраструктур (Интернета) свидетельствуют о том, что эффективное обеспечение кибербезопасности возможно лишь при условии налаживания международного сотрудничества в этой сфере. Это предполагает разработку унифицированного подхода к определению понятия и перечня киберпреступлений и расширение сотрудничества между странами в сфере выявления, пресечения, раскрытия и расследования киберпреступлений. Цели исследования — сформулировать определение понятия «киберпреступность», рассмотреть классификации киберпреступлений и выработать предложения по совершенствованию правового регулирования в сфере противодействия киберпреступности.

Материалы и методы. Объектом исследования являются общественные отношения в сфере противодействия киберпреступности. В процессе исследования этого объекта использовалась юридическая методология, включающая общенаучные, а также специальные научные методы познания.

Результаты исследования. В статье формулируется авторская дефиниция термина «киберпреступность», определяется теоретическое и практическое значение классификаций киберпреступлений, созданных по таким основаниям, как объект преступного посягательства; субъект преступления; способ и средства совершения преступления. В целях повышения эффективности противодействия киберпреступности вносятся конкретные предложения по реформированию российского и международного уголовного законодательства, налаживанию международного сотрудничества в рамках ООН, ШОС, ОДКБ, БРИКС.

Обсуждение и заключения. Выводы, предложения и рекомендации, сформулированные в ходе исследования, обладают определенной теоретической значимостью, так как могут стать основой для дальнейших исследований феномена киберпреступности в рамках уголовного права и криминологии, а также имеют практическое значение для совершенствования практики противодействия киберпреступлениям и повышения эффективности соответствующего уголовного законодательства.

Ключевые слова: киберпреступление, классификация киберпреступлений, криминализация, международное сотрудничество.

Благодарности. Авторы выражают благодарность рецензенту, чья критическая оценка материалов и предложения по их совершенствованию способствовали значительному повышению качества статьи.

Для цитирования. Витвицкая, С. С. Киберпреступления: понятие, классификация, международное противодействие / С. С. Витвицкая, А. А. Витвицкий, Ю. И. Исакова // Правовой порядок и правовые ценности. — 2023. — Т. 1, № 1. — С. 126–136. https://doi.org/10.23947/2949-1843-2023-1-1-126-136

Original article

Cybercrimes: Concept, Classification, International Countering

Svetlana S. Vitvitskaya, Andrey A. Vitvitsky, Yulia I. Isakova

Don State Technical University, 1, Gagarin Sq., Rostov-on-Don, Russian Federation

✉ omar67@yandex.ru

Abstract

Introduction. In the criminal law doctrine, in the legislative sources and internationally recognised official documents there exist different approaches to defining the concepts of "cyber criminality" and "cybercrime", different nomenclatures and classifications of these criminal actions are proposed. These discrepancies negatively influence the efficiency of the fight against this type of crime. The transboundary nature of cybercrimes and interrelation between the information and telecommunication technologies and the information infrastructures (Internet) testify that efficient provision of cybersecurity is possible only on condition of the international cooperation in this field. This implies development of the unified approach to defining the cybercrimes concept and nomenclature and extension of cooperation between the countries in detecting, suppressing, solving and investigating the cybercrimes. The aim of the study is to define the concept of "cyber criminality", to consider cybercrimes classification and to develop proposals for improving the legal regulation in the field of cybercrime countering.

Materials and Methods. The object of the study is social relations in the field of cybercrime countering. In the course of the study, the legal methodology was used, including general as well as special scientific methods.

Results. The article formulates the authors' definition of the term "cyber criminality", defines the theoretical and practical significance of the cybercrimes classification based on the grounds of such notions as: object of criminal encroachment; the subject of the crime; the method and means of committing the crime. Striving to enhance the cyber criminality countering efficiency, the concrete proposals are made to reform the Russian and the international criminal legislation, to establish international cooperation within the framework of the UN, the Shanghai Cooperation Organisation (SCO), the Collective Security Treaty Organisation (CSTO), BRICS.

Discussion and Conclusions. The conclusions, suggestions and recommendations formulated in the course of the study have certain theoretical significance as they can become the basis for further studies of the cyber criminality phenomenon in the frame of the criminal law and criminology, as well as have practical significance for improving the cybercrime countering practices and enhancing efficiency of the relevant criminal legislation.

Keywords: cybercrime, cybercrimes classification, criminalisation, international cooperation.

Acknowledgements. The authors express their gratitude to reviewer, whose critical assessment of the materials and suggestions for their improvement contributed to significant improvement of article's quality.

For citation. S. S. Vitvitskaya, A. A. Vitvitsky, Y. I. Isakova. Cybercrimes: Concept, Classification, International Countering. Legal Order and Legal Values, 2023, vol. 1, no 1, pp. 126–136. https://doi.org/10.23947/2949-1843-2023-1-1-126-136

Введение. Киберпреступность является относительно новой, однако чрезвычайно опасной и динамично развивающейся разновидностью преступности, имеющей трансграничный, высокоинтеллектуальный, организованный характер, угрожающей самым различным правоохраняемым ценностям (личности, обществу, государству). Трансграничный характер киберпреступлений и взаимосвязанность информационно-телекоммуникационных технологий и информационных инфраструктур (Интернета) свидетельствуют о том, что эффективное обеспечение кибербезопасности возможно лишь при условии налаживания международного сотрудничества в этой сфере. Это предполагает как разработку унифицированного подхода к определению понятия киберпреступности и перечня киберпреступлений, так и налаживание взаимодействия между странами в сфере выявления, пресечения, раскрытия и расследования киберпреступлений. Цель настоящего исследования — сформулировать определение понятия «киберпреступность», рассмотреть классификации киберпреступлений и выработать предложения по совершенствованию правового регулирования в сфере противодействия киберпреступности.

Материалы и методы. Объектом исследования являются общественные отношения в сфере противодействия киберпреступности. В процессе исследования этого объекта использовалась юридическая методология, включающая разнообразные приемы, формы и способы познания, среди которых выделяются: общенаучные методы исследования (анализ и синтез, структурно-системный и функциональный подходы), а также специальные научные методы, в том числе историко-политический, компаративистский, конкретно-социологический, формально-логический, систематический, грамматический и др.

В юридической и иной научной литературе для обозначения общественно-опасных деяний, осуществляемых с использованием информационно-телекоммуникационных технологий, используются различные термины и формулировки. Это «компьютерные преступления», «киберпреступления», «интернет-преступления», «преступления, совершаемые с использованием интернет-технологий», «преступления, совершаемые в виртуальной среде», «преступления, совершаемые в Интернете», «преступления, совершаемые с помощью информационно-телекоммуникационных технологий», «компьютерная преступность», «киберпреступность», «интернет-преступность», «кибератаки», «кибервойны», «киберконфликты» и др. Содержание каждой из вышеперечисленных категорий подвергается обсуждению и интерпретации.

Анализ научных источников, официальных документов и нормативных правовых актов, посвященных проблеме противодействия деяниям, совершаемым с использованием информационно-телекоммуникационных технологий, показывает, что одни правоведы склонны узко трактовать содержание вышеперечисленных дефиниций, сводя их к посягательствам на такой правоохраняемый объект, как информационная безопасность [1–4]. В рамках «широкого» подхода вышеуказанные термины используются для обозначения самых различных преступлений, совершаемых в виртуальном (Интернет) пространстве [5, 6] с использованием компьютерной

техники и информационно-телекоммуникационных сетей, а также иных средств доступа к киберпространству [7–9].

По нашему мнению, широкое толкование терминов является правомерным. Результаты криминологических исследований свидетельствуют о наличии устойчивой тенденции к появлению в виртуальном пространстве все новых видов посягательств на различные правоохраняемые общественные отношения, ценности, права и свободы. Объектами преступлений становятся жизнь, здоровье, нравственное, физическое, половое развитие несовершеннолетних. Преступники посягают на собственность, в том числе и интеллектуальную, на общественную безопасность, общественный порядок, общественное здоровье, общественную нравственность, основы конституционного строя и государственной власти, мир и безопасность человечества. Для киберпреступлений характерно то, что информация, информационно-телекоммуникационные технологии могут выступать предметом, орудием или средством совершения общественно-опасного деяния [10].

На международном уровне тенденция к широкому толкованию анализируемых нами понятий обнаружила себя при обсуждении актуальных проблем противодействия киберпреступлениям в рамках X Конгресса ООН, который состоялся в 2000 г. [11]. Эксперты использовали понятие киберпреступности на этом симпозиуме для обозначения «компьютерных» преступлений, где объектом является информационная безопасность, а предметом — компьютер, а также посягательств на любые общественные отношения, совершаемых с использованием компьютеров в качестве орудия или средства.

Первым международно-правовым актом, в котором были приняты меры к унификации перечня и признаков киберпреступлений, стала Конвенция о киберпреступности, принятая Комитетом министров Совета Европы 8 ноября 2001 г. в г. Будапешт [12]. По состоянию на октябрь 2022 года этот нормативный акт ратифицировали 67 государств, в том числе Австралия, Канада, Соединенные Штаты, Израиль, Япония, Аргентина, Гана, Доминиканская Республика, Кабо–Верде, Колумбия, Коста-Рика, Маврикий, Марокко, Нигерия, Панама, Парагвай, Перу, Сенегал, Филиппины, Чили, Шри-Ланка, Тонга.

В этом документе государствам-участникам предлагается криминализировать посягательства на такие объекты, как информационная (компьютерная) безопасность, собственность, интеллектуальная собственность, а также деяния, связанные с распространением незаконного контента в информационных сетях (детская порнография; информация экстремистского характера). Подобная трактовка киберпреступности прослеживается и в других директивах стран-участниц Конвенции, которые были посвящены проблемам противодействия атакам на информационные сети, а также сохранению безопасности сетей и информационных систем.

Таким образом, в вышеуказанных документах ООН и Евросоюза к киберпреступности причисляются не только «компьютерные» преступления, посягающие на информационную безопасность, но и иные преступления, использующие компьютер как орудие (computer-facilitated) либо средство преступления (computer-related). Думается, эта позиция является в целом правильной, так как использование информационно-телекоммуникационных технологий в качестве орудия или средства преступного посягательства на любые объекты повышает эффективность преступной деятельности, придавая ей качественно новую форму, делая ее трансграничной, масштабной и труднораскрываемой. К сожалению, в указанных выше документах ООН и Евросоюза ничего не говорится о противодействии использованию информационно-телекоммуникационных технологий в качестве оружия в военно-политических конфликтах, для вмешательства во внутренние дела государств, для осуществления подрывной, террористической, шпионской и диверсионной деятельности.

Кроме того, в анализируемых официальных актах ООН и Евросоюза не учитываются возможности «мобильного» доступа в Интернет для совершения киберпреступлений. Это не позволяет относить к

киберпреступлениям посягательства, при совершении которых используются не компьютерные, а иные устройства, обеспечивающие доступ к сети, в частности «портативные» мобильные телефоны. Поэтому правильнее было бы считать, что киберпреступность представляет собой совокупность преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, посягающих на информационную безопасность и(или) использующих компьютер, а также иные устройства, обеспечивающие доступ к сети, в качестве орудия либо средства совершения преступления.

Следует отметить, что большинство стран, в том числе Россия, Китай, Индия и Бразилия, признавая необходимость налаживания противодействия киберпреступности на международном уровне, не подписали конвенцию Совета Европы 2001 г. Разногласия со странами-участницами возникли относительно статьи 32 (параграф b) «о трансграничном доступе к компьютерным данным», позволяющей различным спецслужбам без официального уведомления проводить операции в компьютерных сетях третьих стран. Эксперты в области информационно-телекоммуникационных технологий считают, что подобное право существенно угрожает безопасности государств, нарушает цифровой суверенитет стран, узурпирует право на конфиденциальность персональных данных. По мнению экс-сотрудник ЦРУ Эдварда Сноудена, эта норма является отражением киберполитики США, которая делает ставку не на защиту от киберпреступлений, а на шпионаж и взлом сетей других стран [13].

Для такого рода подозрений есть объективные основания. Если обратиться к истории возникновения и развития информационных систем и сетей, то следует обратить внимание на то, что прообраз Интернета был разработан в целях налаживания внутриведомственного взаимодействия в оборонных и разведывательных структурах США, которые впоследствии (не без задней мысли) дали ему путевку в «большую жизнь». Как известно, США активно использовали информационно-телекоммуникационные технологии для установления слежки за своими и иностранными гражданами, сбора персональных данных и сведений составляющих личную или семейную тайну, и последующего установления контроля над лицами, занимающими ключевые государственные должности или занимающимися политической деятельностью; для распространения сепаратистского и экстремистского контента; организации «оранжевых» революций.

То же самое можно сказать о происхождении анонимайзеров. Например, TOR (The Onion Router) был разработан ВМС США. В 2002 г. эта программа была рассекречена и передана независимым разработчикам, которые создали клиентское программное обеспечение и опубликовали исходный код под свободной лицензией, чтобы все желающие могли его опробовать. Ныне TOR активно используется преступными элементами для различной противоправной деятельности в черном сегменте Интернета — Даркнете (darknet), в том числе для торговли наркотическими средствами, психотропными веществами, оружием, боеприпасами, взрывчатыми веществами, для организации и проведения незаконных азартных игр, торговли людьми, распространения порнографических изображений несовершеннолетних, торговли персональными данными. При помощи этого сегмента организуются хакерские аукционы, на которых продаются новейшие разработки, обеспечивающие противоправный доступ, копирование, модификацию и уничтожение компьютерной информации в целях хищения, совершения атак на объекты инфраструктуры. Проводя свою агрессивную политику в информационной сфере, США в целях удержания цифрового доминирования, пытаются лоббировать распространение американских компьютерных и иных телекоммуникационных устройств, компьютерных программ; популяризировать американские социальные сети; инициировать принятие нормативных актов, в том числе и на международном уровне, с помощью которых они могут получить доступ к информационным данным любых лиц, организаций и государств, и использовать их в разведывательных, контрразведывательных,

подрывных целях.

Пытаясь замаскировать свои намерения, США в документах стратегического планирования, посвященных обеспечению информационной безопасности, последовательно обвиняют другие страны (прежде всего, Россию и Китай) в кибернападениях; угрожают применением любого, в том числе ядерного оружия в случаях посягательств на их информационную инфраструктуру; составляют лжерейтинги свободы использования Интернета, в которых первые места, разумеется, отдаются западным странам, а последние — государствам, пытающимся отстоять свой цифровой суверенитет; активно задействуют для кибернападений и кибершпионажа частные IT-фирмы и даже отдельных хакеров. То же самое делают другие страны коллективного Запада (Евросоюз, Великобритания, Австралия, Канада и др.). В частности, в стратегиях обеспечения информационной безопасности Евросоюза указываются те же источники угроз, что и в подобных документах США — Россия и Китай. В проводимых учениях по обеспечению кибербезопасности разыгрываются сценарии отражения кибератак со стороны Китая и России.

Несмотря на этот неконструктивный, и прямо скажем, агрессивный настрой недружественных стран, Россия и целый ряд государств, входящих в ШОС, БРИКС, АТЭС, СНГ, ОДКБ, пытаются последовательно отстаивать свое видение равноправных отношений в информационной сфере, исключающее доминирование одних стран над другими, гарантирующее цифровой суверенитет различных государств, обеспечивающее использование информационно-телекоммуникационных средств и сетей только в конструктивных целях, во благо всего мира и человечества.

Примером этого являются законодательные инициативы перечисленных выше международных организаций. Так, в 2011 г. члены ШОС — Россия, Китай, Узбекистан, Таджикистан — разработали и представили Генеральному Секретарю ООН «Правила поведения государств в области обеспечения международной информационной безопасности», в которых указывается на потребность в интернационализации управления сетью Интернет, подчеркивается необходимость установления запретов относительно применения государствами компьютерных и иных коммуникационных средств в целях совершения посягательств на международный мир и безопасность, вмешательства во внутреннюю политику иных стран, использования военной силы для разрешения международных киберконфликтов.

Страны БРИКС (Бразилия, Индия, Китай, Россия, ЮАР) в 2014 г. приняли Форталезскую декларацию, в которой указывается на необходимость налаживания широкого международного сотрудничества (в рамках ООН) в сфере противодействия киберпреступности и заявляется о недопустимости использования информационно-телекоммуникационных технологий для кибернападений на объекты стратегического назначения, финансового сектора, атомной энергетики и т.п.

В 2016 году в ООН был принят проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», представленной 80 государствами, в том числе странами БРИКС. В этом документе была поставлена задача выработки основ ответственного поведения государств в информационном пространстве и преодоления разрыва в уровне развития ИКТ между развитыми и развивающимися странами.

В 2020 г. на саммите Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) обсуждались вопросы координации мер по защите персональной информации и борьбе с киберпреступлениями.

Существенную роль в создании и наращивании потенциала информационной безопасности может сыграть создание кризисных центров ОДКБ, ШОС, БРИКС для совместного реагирования на серьезные киберугрозы, включая атаки на критическую инфраструктуру государств-участников, отработка сценариев урегулирования

международных кризисов в виртуальном пространстве.

В 2021 г. Россия внесла в ООН проект Конвенции о противодействии использованию ИКТ в преступных целях [14], в котором исключен пункт о трансграничном доступе к хранящимся компьютерным данным; приведен перечень деяний, совершенных в Интернете; указано на возможность использования телефона и других средств коммуникаций при совершении киберпреступлений. Круг киберпреступлений в этом законопроекте существенно расширен по сравнению с Европейской Конвенцией. К киберпреступлениям отнесены посягательства на критическую информационную инфраструктуру; склонение к самоубийству или доведение до его совершения; вовлечение несовершеннолетнего в совершение противоправных действий, опасных для его жизни и здоровья; деяния в сфере незаконного оборота наркотических средств, психотропных веществ, фальсифицированных лекарственных средств и медицинских изделий, оружия; подстрекательство к подрывной или вооруженной деятельности; преступления террористической направленности; оправдание преступлений против мира и человечности и нацизма; использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом и др.

На наш взгляд, российскую законодательную инициативу следует признать весьма своевременной и разумной. Дело в том, что с момента принятия Будапештской конвенции криминологическая ситуация в киберпространстве существенно изменилась. С использованием телекоммуникационных технологий совершаются деяния, нацеленные на ослабление морально-нравственных основ общества, на дестабилизацию демографической и психологической ситуации в странах-оппонентах, на ведение информационной войны. Наблюдается такая форма киберпреступления, как кибершпионаж. Существует реальная угроза употребления информационно-телекоммуникационных технологий в ходе внешнеполитических и военных конфликтов для осуществления диверсий на объектах критической информационной инфраструктуры и др. Появились новые формы киберпосягательств на общественную безопасность, здоровье населения, общественную нравственность и другие правоохраняемые объекты.

Представляется, что российское национальное уголовное законодательство нуждается в реформировании для повышения эффективности противодействия киберпреступности. В частности, в УК РФ следует криминализировать новые виды преступлений против цифровой безопасности (несанкционированный доступ к персональным данным; незаконный оборот устройств, разработанных или адаптированных для целей совершения преступлений и др.). В качестве обстоятельства, отягчающего наказание, в ст. 63 УК РФ следует упомянуть совершение преступления с использованием информационно-телекоммуникационных технологий. Помимо этого необходимо осуществлять постоянный мониторинг криминологической ситуации, нацеленный на выявление новых видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, проводить дальнейшие научные исследования этих общественно-опасных деяний, заниматься их всесторонним анализом и классификацией.

В настоящее время существуют различные классификации киберпреступлений, созданные по разным основаниям. По объекту деяния, совершаемые с использованием информационно-телекоммуникационных технологий, подразделяются преступления против жизни и здоровья несовершеннолетних; против собственности, интеллектуальной собственности; общественной безопасности; общественного порядка; здоровья населения; общественной нравственности; компьютерной безопасности; против основ конституционного строя и безопасности государства, мира и безопасности человечества и др. Данная классификация имеет значение для правильной систематизации соответствующих новелл в рамках действующего уголовного закона.

В зависимости от субъекта деяния следует подразделить преступления, совершаемые физическими лицами, с использованием информационно-телекоммуникационных технологий, в том числе лицами, выполняющими управленческие функции или исполняющими должностные обязанности, а также общественно опасные деяния, совершаемые одними государствами против других. Данная классификация играет важную роль для решения вопросов установления различных видов ответственности в рамках национального уголовного законодательства и международно-правовых договоров. Отметим, что еще в 2017 г. отечественный Центр стратегических разработок (ЦСР) выступил с инициативой, касающейся адаптации ключевых норм международного гуманитарного права, в том числе Женевских конвенций, к общественно опасным действиям государств с использованием информационно-телекоммуникационных технологий.

Классификации киберпреступлений по способу и средствам совершения преступления имеют важное криминологическое и криминалистическое значение. В качестве примера приведем «Рекомендательные типологии новых преступлений, совершаемых с использованием информационных технологий», разработанные Межпарламентской Ассамблеей государств-участников Содружества Независимых Государств [15]. В постановлении № 51-24 от 27 ноября 2020 года отмечается, что неконкретность понятий и отсутствие единого подхода к терминологии и классификации новых способов совершения преступлений в сфере информационных технологий осложняет противодействие им, а предлагаемая типология дает возможность создать единый механизм учетно-аналитических операций при оценке состояния и динамики киберпреступности и определить пути сотрудничества в рассматриваемой сфере. Авторы этого документа выделяют следующие виды киберпреступлений: 1) мошеннические действия с использованием сети Интернет, средств подвижной связи и систем дистанционного банковского обслуживания; 2) хищения через вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем подделки электронных средств идентификации платежей, использования идентификационных данных банковских карт; 3) иные способы хищений и причинения имущественного ущерба посредством использования средств подвижной связи (взимание повышенных сборов за телефонные звонки, мошенничество на платформах бесплатных объявлений, мошенничество в виде конкурса СМС-сообщений или теста на общие знания); 4) использование информационных технологий для совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров; 5) использование информационных технологий с целью совершения преступлений против несовершеннолетних, в том числе склонение несовершеннолетних к совершению самоубийства, вовлечение их в порнобизнес; 6) использование информационных технологий для совершения преступлений террористического и экстремистского характера, в том числе кибертерроризма. В указанном постановлении Межпарламентской Ассамблеи СНГ представлен развернутый анализ преступных схем и методик. Это позволит существенно повысить эффективность предупреждения, пресечения, раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий на национальном уровне и наладить взаимодействие правоохранительных органов государств-союзников в данных сферах, в том числе организовать информационный обмен, скоординировать правовые, организационные и технические меры противодействия.

Результаты исследования. Киберпреступность представляет собой совокупность преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, посягающих на информационную безопасность и(или) использующих компьютер, а также иные устройства, обеспечивающие доступ к сети, в качестве орудия (computer-facilitated) либо средства преступления (computer-related).

Необходимо осуществлять постоянный мониторинг криминологической ситуации, нацеленный на выявление

новых видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, проводить дальнейшие научные исследования этих общественно опасных деяний, заниматься их всесторонним анализом и классификацией с целью своевременной криминализации новых видов общественно опасных деяний, разработки наиболее эффективных мер противодействия им.

Классификации киберпреступлений, созданные по различным основаниям, имеют разное прикладное значение. Классификация по объекту преступного посягательства играет важную роль для правильной систематизации соответствующих новелл в рамках действующего уголовного закона. Классификация в зависимости от субъекта преступного деяния имеет значение для решения вопросов установления различных видов ответственности в рамках национального уголовного законодательства и международно-правовых договоров. Классификации по способу и средствам совершения преступления имеют важное криминологическое и криминалистическое значение.

В целях повышения эффективности противодействия киберпреступности российское национальное уголовное законодательство нуждается в реформировании. В УК РФ следует криминализировать новые виды преступлений против цифровой безопасности (несанкционированный доступ к персональным данным; незаконный оборот устройств, разработанных или адаптированных для целей совершения преступлений и др.); а в качестве обстоятельства, отягчающего наказание, в ст. 63 УК РФ следует упомянуть «совершение преступления с использованием информационно-телекоммуникационных технологий».

Трансграничный характер киберпреступлений и взаимосвязанность информационно-телекоммуникационных технологий и информационных инфраструктур (прежде всего, Интернета) свидетельствуют о том, что эффективное обеспечение кибербезопасности возможно лишь при условии налаживания международного сотрудничества в этой сфере. Это предполагает разработку унифицированного подхода к определению понятия и перечня киберпреступлений, и расширения сотрудничества между странами в сфере выявления, пресечения, раскрытия и расследования киберпреступлений.

В условиях современного острого внешнеполитического противостояния стран коллективного Запада, с одной стороны, России и ее союзников, с другой стороны, противодействие общественно опасным деяниям, совершаемым с использованием информационно-телекоммуникационных технологий, осуществляется преимущественно на уровне блоков отдельных государств.

Создание коллективных форм взаимодействия в сфере обеспечения информационной безопасности возможно с союзниками и партнерами России (в рамках ОДКБ, ШОС, БРИКС) на основе согласования общих принципов, норм и правил поведения в киберсреде; унификации норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые в виртуальном пространстве; налаживания взаимодействия в области информационного обмена, предупреждения, выявления, пресечения, раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий; создания механизмов коллективной обороны от киберагрессии со стороны недружественных государств.

Существенную роль в создании и наращивании потенциала информационной безопасности может сыграть создание кризисных центров ОДКБ, ШОС, БРИКС для совместного реагирования на серьезные киберугрозы, включая атаки на критическую инфраструктуру государств-участников, отработка сценариев урегулирования международных кризисов в виртуальном пространстве.

Обсуждение и заключения. Выводы, предложения и рекомендации, сформулированные в ходе исследования, способствуют достижению цели повышения эффективности противодействия киберпреступности. Теоретическая значимость выводов заключается в том, что представленные положения

могут стать основой для дальнейших исследований феномена киберпреступности в рамках уголовного права и криминологии. Результаты исследования имеют определенное практическое значение для повышения эффективности соответствующего уголовного законодательства и совершенствования деятельности в сфере предупреждения и пресечения киберпреступлений.

Список литературы

1. Гасанов, А. М. Понятие и признаки киберпреступлений / А. М. Гасанов, Я. Ю. Меженина // Colloquium-Journal. — 2019. — № 16–7 (40). — С. 137–138.

2. Рябинин, К. Ю. Понятие и признаки киберпреступлений / К. Ю. Рябинин // Colloquium-Journal. — 2020. — № 5–8 (57). — С. 46–48.

3. Голубев, В. А. «Кибертерроризм» — миф или реальность? Центр исследования компьютерных преступлений / В. А. Голубев // Computer Crime Research Centre : [сайт]. — URL: http://www.crime-research.org/ (дата обращения: 15.12.2022).

4. Кучерков, И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. — 2019. — № 10. — С. 78–81.

5. Романов, И. В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. — 2016. — № 5 (13). — С. 105–109.

6. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. … канд. юрид. наук / Т. Л. Тропина. — Владивосток, 2005. — 28 с.

7. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. … канд. юрид. наук / М. А. Простосердов. — Москва, 2016. — 232 с.

8. Ищенко, Е. П. О криминалистическом обеспечении раскрытия и расследования киберпреступлений / Е. П. Ищенко // Деятельность правоохранительных органов в современных условиях : сборник материалов 20-й международной научно-практической конференции. В 2 томах. Том 1. — Иркутск : Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2015. — С. 336–341.

9. Киберпреступность — определение, классификация киберпреступлений. — URL: https://elcomrevue.ru/blog/cybercrime/kibeoprestupnost-chto-eto/ (дата обращения: 15.12.2022).

10. Номоконов, В. А. Киберпреступность, как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология. Вчера. Сегодня. Завтра. — 2012. — № 1 (24). — С. 45–55.

11. Волеводз, А. Г. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями: сборник документов / А. Г. Волеводз. — Москва : Изд-во «Юрлитинформ», 2001. — 496 с.

12. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // СПС Гарант : [сайт]. — URL: https://base.garant.ru/4089723/ (дата обращения: 21.12.2022).

13. Киберпреступность в мире // Портал TAdviser : [сайт]. — URL: https:// www.tadviser.ru (дата обращения: 21.12.2022).

14. Проект Конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях по борьбе с киберпреступностью. — URL:https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_R.pdf (дата обращения: 21.12.2022).

15. О Рекомендательных типологиях новых преступлений, совершаемых с использованием информационных

технологий: Постановление межпарламентской Ассамблеи государств-участников СНГ от 27 ноября 2020 г. № 51-24 // СПС Гарант : [сайт]. — URL: https://base.garant.ru/4089723/ (дата обращения: 21.12.2022).

Поступила в редакцию 15.01.2023.

Поступила после рецензирования 01.02.2023.

Принята к публикации 03.02.2023

Об авторах:

Витвицкая Светлана Сергеевна, доцент кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат юридических наук, доцент, ORCID, omar67@yandex.ru

Витвицкий Андрей Анатольевич, доцент кафедры «Гражданское право» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат юридических наук, доцент, ORCID, fishbrook@yandex.ru

Исакова Юлия Игоревна, декан факультета «Юридический», заведующий кафедрой «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), доктор социологических наук, кандидат юридических наук, доцент, ORCID, isakova.pravo@bk.ru

Заявленный вклад соавторов:

А. А. Витвицкий — формирование основной концепции, определение целей и задач, методологии исследования. С. С. Витвицкая — подготовка текста, формирование выводов. Ю. И. Исакова — анализ результатов исследования, доработка текста, корректировка выводов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.